CLAIMS

What is claimed is:

1. A user authentication method that authenticates a user based on a graphical password input by the user, the user authentication method comprising:

determining whether the graphical password has been input;

determining whether to authenticate the user depending on whether the extent to which a location of the input graphical password matches with a reference location of a registered graphical password is within an authentication margin for a location of any input graphical password with respect to the reference location of the registered graphical password;

storing a graphical password input history if the user is not authenticated;

determining whether there has been an intrusion by referring to the graphical password input history; and

reducing the authentication margin if determined that there has been an intrusion.

2. The user authentication method of claim 1, wherein the reference location of the registered graphical password is a predetermined area.

3. The user authentication method of claim 1, wherein the determining whether to authenticate the user further comprises determining whether an order of received graphical passwords matches with an order of registered graphical passwords.

4. The user authentication method of claim 1, wherein the determining whether there has been an intrusion comprises referring to the graphical password input history and checking if a graphical password has been input beyond a predetermined distance from the reference location of the registered graphical password.

5. The user authentication method of claim 1, further comprising displaying a background picture on the screen of the terminal.

6. The user authentication method of claim 1, further comprising restoring the reduced authentication margin if the determination that there has been an intrusion is cancelable based on the graphical password input history.

7. A user authentication method that authenticates a user based on biometrics information and a graphical password input by the user, the user authentication method comprising:

determining whether the graphical password has been input;

variably setting a threshold value of biometrics depending on the extent to which the input graphical password matches with a registered graphical password; and

determining whether to authenticate the user based on a result of comparing the user's biometrics information with registered biometrics.

8. The user authentication method of claim 7, wherein the variably setting the threshold value of biometrics comprises:

determining whether to authenticate the user depending on the extent to which the input graphical password matches with the registered graphical password; and

variably setting the threshold value of biometrics depending on the extent to which the input graphical password matches with the registered graphical password.

9. The user authentication method of claim 8, wherein the determining whether to authenticate the user comprises:

determining whether to authenticate the user depending on whether the extent to which a location of the input graphical password matches with a reference location of the registered graphical password is within an authentication margin;

storing a graphical password input history if the user is not authenticated based on the input graphical password;

determining whether there has been an intrusion by referring to the graphical password input history; and

reducing the authentication margin if determined that there has been an intrusion.

10. The user authentication method of claim 9, wherein the reference location of the registered graphical password is a predetermined area.

11. The user authentication method of claim 9, wherein the determining whether to authenticate the user further comprises, determining whether an order of received graphical passwords matches with an order of registered graphical passwords.

12. The user authentication method of claim 9, wherein the determining whether there has been an intrusion comprises checking if a graphical password has been input beyond a predetermined distance from the reference location of the registered graphical password.

13. The user authentication method of claim 9, further comprising:

restoring the reduced authentication margin if the determination that there has been an intrusion is cancelable based on the graphical password input history.

14. The user authentication method of claim 7, further comprising displaying a background picture on the screen of the terminal.

15. The user authentication method of claim 7, further comprising:

storing a graphical password input history ; and

determining whether there has been an intrusion by referring to the graphical password input history if the user is not authenticated.

16. The user authentication method of claim 15, further comprising:

storing an intruder's biometrics if determined that there has been an intrusion, wherein the user is authenticated depending on a result of comparing the user's biometrics information with the stored intruder's biometrics information.

17. The user authentication method of claim 7, further comprising:

storing a graphical password input history; and

varying a variation range of the threshold value using the graphical password input history if the user is not authenticated.

18. The user authentication method of claim 17, wherein, the variation range of the threshold value is varied so as to increase the level of security if an incorrect graphical password has been input at least n times.

19. The user authentication method of claim 18, wherein the varying the variation range o the threshold value comprises restoring the varied variation range of the threshold value if the graphical password has been input m times or more correctly since the variation range of the threshold value was varied.

20. The user authentication method of claim 7, further comprising:

adding/renewing an authentication key if the user is authenticated.

21. The user authentication method of claim 20, wherein, the authentication key is added/renewed only when the input graphical password matches with the registered graphical password and the user is authenticated.

22. The user authentication method of claim 20, wherein in step (h), the authentication key is added/renewed only when the user is authenticated and the extent to which the user's biometrics information matches with the registered biometrics information is larger than a predetermined threshold value.

23. A user authentication apparatus that authenticates a user based on a graphical password input by the user, the user authentication apparatus comprising:

a graphical password input unit which determines whether the graphical password has been input;

a control unit which determines whether to authenticate the user depending on whether the extent to which a location of the input graphical password matches with a reference location of a registered graphical password is within an authentication margin for a location of any input graphical password with respect to the reference location of the registered graphical password;

a storage unit which stores the registered graphical password and stores a graphical password input history if the user is not authenticated; and

a graphical password input history analysis unit which determines whether an intrusion occurred by referring to the graphical password input history,

wherein the control unit reduces the authentication margin of the location of any input graphical password with respect to the reference location of the registered graphical password if the graphical password input history analysis unit determines that there has been an intrusion.

24. The user authentication apparatus of claim 23, wherein the reference location of the registered graphical password is a predetermined area.

25. The user authentication apparatus of claim 23, wherein the control unit determines whether to authenticate the user depending on whether graphical passwords have been input in a right order.

26. The user authentication apparatus of claim 23, wherein the graphical password input history analysis unit determines that there has been an intrusion if a graphical password has been input beyond a predetermined distance from the reference location of the registered graphical password.

27. The user authentication apparatus of claim 23, further comprising a display unit which displays a background picture on the screen of the terminal.

28. The user authentication apparatus of claim 23, wherein the control unit resets the reduced authentication margin if the determination that there has been an intrusion is cancelable based on the graphical password input history.

29. A user authentication apparatus that authenticates a user based on biometrics information and a graphical password input by the user, the user authentication apparatus comprising:

a graphical password input unit which determines whether the graphical password has been input;

a storage unit which stores registered graphical password and registered biometrics information;

a control unit which variably sets a threshold value of biometrics depending on the extent to which the input graphical password matches with the registered graphical password; and

a biometrics unit which determines whether to authenticate the user based on a result of comparing the user's biometrics information input from the outside with registered biometrics.

30. The user authentication apparatus of claim 29, wherein the control unit determines whether to authenticate the user, depending on the extent to which the input graphical password matches with the registered graphical password, and variably sets the threshold value for living body recognition, depending on the extent to which the input graphical password matches with the registered graphical password.

31. The user authentication apparatus of claim 30, wherein the control unit determines whether to authenticate the user, depending on whether the extent to which a location of the input graphical password matches with a reference location of the registered graphical password is within an authentication margin, determines whether there has been an intrusion by referring to the graphical password input history, and reduces the authentication margin if determined that there has been an intrusion, and the storage unit stores the graphical password input history if the user is not authenticated based on the input graphical password.

32. The user authentication apparatus of claim 31, wherein the reference location of the registered graphical password is a predetermined area.

33. The user authentication apparatus of claim 31, wherein the control unit determines whether to authenticate the user depending on whether an order of received graphical passwords matches with an order of registered graphical passwords.

34. The user authentication apparatus of claim 31, wherein the control unit determines that there has been an intrusion if the graphical password has been input beyond a predetermined distance from the reference location of the registered graphical password.

35. The user authentication apparatus of claim 31, wherein the control unit restores the reduced authentication margin if the determination that there has been an intrusion is considered as being cancelable based on the graphical password input history.

36. The user authentication apparatus of claim 29, further comprising a display unit which displays a background picture on the screen of the terminal.

37. The user authentication apparatus of claim 29, wherein the storage unit stores the graphical password input history, and the control unit determines whether there has been an intrusion by referring to the graphical password input history if the user is not authenticated.

38. The user authentication apparatus of claim 37, wherein the storage unit stores an intruder's biometrics if the graphical password input history analysis unit determines that there has been an intrusion, and the biometrics unit determines whether to authenticate the user depending on a result of comparing the user's biometrics information with the intruder's biometrics information stored in the storage unit.

39. The user authentication apparatus of claim 29, wherein the storage unit stores the graphical password input history, and the control unit varies a variation range of the threshold value using the graphical password input history if the user is not authenticated.

40. The user authentication apparatus of claim 39, wherein the control unit varies the variation range of the threshold value so as to increase the level of security if an incorrect graphical password has been input n times or more.

41. The user authentication apparatus of claim 40, wherein the control unit restores the varied variation range of the threshold value if a right graphical password has been input m times or more since the variation range of the threshold value was varied.

42. The user authentication apparatus of claim 29, wherein an authentication key is added/renewed if the user is authenticated by the biometrics unit.

43. The user authentication apparatus of claim 42, wherein the authentication key is added/renewed only when the user is authenticated by the biometrics unit and the input graphical password matches with the registered graphical password.

44. The user authentication apparatus of claim 42, wherein the authentication key is added/renewed only when the user is authenticated and the extent to which the user's biometrics information matches with the registered biometrics information is larger than a predetermined threshold value.

45. A computer-readable recording medium on which a program enabling the user authentication method of claim 1 is recorded.

46. A computer-readable recording medium on which a program enabling the user authentication method of claim 7 is recorded.

47. A user authentication method, comprising:

comparing an input graphical password to a registered graphical password and outputting a valid result when the input graphical password is within a predetermined proximity window of the registered graphical password and outputting an invalid result when the input graphical password is outside the predetermined proximity window of the registered graphical password, wherein the user is authenticated when the valid result is output; and

adjusting the predetermined proximity window, wherein the predetermined proximity window is decreased when the invalid result is output.

48. The method of claim 47, further comprising:

comparing the user's input biometric information to registered biometric information using a predetermined threshold level which corresponds to a predetermined false acceptance rate and a predetermined false rejection rate.

49. The method of claim 48, wherein the predetermined threshold level is set so that the false rejection rate is reduced when the valid result is output and the false acceptance rate is reduced when the invalid result is output.

50. The method of claim 48, further comprising:

counting a number of invalid result outputs; and

storing the user's biometric information as intruder biometric information when the number exceeds a predetermined intruder count level.

51. The method of claim 50, further comprising:

comparing the user's biometric information to the intruder biometric information and blocking the user when there is a match.

52. A method of user authentication, comprising:

authenticating a user by adjusting a biometric threshold based on comparing an input graphical password to an authorized graphical password, wherein the threshold is set to increase the possibility of the user being authenticated when the input graphical password matches the authorized graphical password and the threshold is set to decrease the possibility of the user being authenticated when the input graphical password does not match the authorized graphical password.

53. The method of claim 52, wherein the input graphical password matches the authorized graphical password when the input graphical password is within a predetermined proximity of the authorized graphical password.

54. A user authentication apparatus, comprising:

a graphical password input unit which receives a graphical password input by a user, wherein a key manipulation unit is not used to input the graphical password;

a storage unit which stores registered graphical password and registered biometrics information corresponding to authorized users;

a control unit which variably sets a threshold biometrics value depending on the degree to which the input graphical password is proximate to the registered graphical password; and

a biometrics unit which reads the user's biometrics information and determines whether to authenticate the user based on a result of comparing the user's biometrics information with the registered biometrics using the set threshold biometrics value.

55. The apparatus of claim 54, wherein the control unit sets the threshold biometrics value to lower a false acceptance rate when the input graphical password is outside a predetermined proximity area of the registered graphical password and sets the threshold biometrics value to lower a false rejection rate when the input graphical password is within the predetermined proximity area of the registered graphical password.